Secure Two-Way RFID Communications

ABSTRACT OF THE DISCLOSURE

Methods and apparatus for providing secure two-way (reader-to-tag and tag-to-reader) RFID communications. According to one aspect of the invention, a tag receives a noise-encrypted RF carrier signal from a reader and backscatter modulates it with tag information. Eavesdroppers cannot extract the tag information from the backscattered signal because it is masked by the noise encryption. According to another aspect of the invention, establishing a secure two-way RFID communication link includes a reader modulating a carrier signal with a noise encryption signal and broadcasting the noise-encrypted carrier to a singulated tag. The tag backscatter modulates the noise-encrypted carrier with a first portion of a key and/or a one-time pad pseudorandom number. If a key is used, upon receiving the backscattered signal the reader verifies that the tag is authentic, and, if verified as authentic, transmits a second portion of the key, possibly encrypted by a function depending on the one-time pad pseudorandom number, to the tag.